Enhancing Security of MME Handover via Fractional Programming and Firefly Algorithm

Quoc-Tuan Vien, *Senior Member, IEEE,* Tuan Anh Le, *Senior Member, IEEE,* Xin-She Yang, Trung Q. Duong, *Senior Member, IEEE,*

***Abstract*—Key update and residence management have been investigated as an effective solution to cope with desynchronisation attacks in Mobility Management Entity (MME) handovers. In this paper, we first analyse the impacts of the Key Update Interval (KUI) and MME Residence Interval (MRI) on handover processes and their secrecy performance in terms of the Number of Exposed Packets (NEP), Signaling Overhead Rate (SOR) and Outage Probability of Vulnerability (OPV). Specifically, the bounds of the derived NEP and SOR not only capture their behaviours at the boundary of the KUI and MRI, but also show the trade-off between the NEP and SOR. Additionally, through the analysis of the OPV, it is shown that the handover security can be enhanced by shortening the KUI and the desynchonisation attacks can be avoided with high-mobility users. The above facts accordingly motivate us to propose a Multi-objective Optimisation (MO) problem to find the optimal KUI and MRI that minimise both the NEP and SOR subject to the constraint on the OPV. To this end, two scalarisation techniques are adopted to transform the proposed MO problem into single-objective optimisation problems, i.e., an achievement-function method via Fractional Programming (FP) and a weighted-sum method. Based on the derived bounds on NEP and SOR, the FP approach can be optimally solved via a simple numerical method. For the weighted-sum method, the Firefly Algorithm (FA) is utilised to find the optimal solution. The results show that both techniques can solve the proposed MO problem with a significantly reduced searching complexity compared to the conventional heuristic iterative search technique.**

***Index Terms*—Handover security; desynchronisation attacks; multiobjective optimisation; firefly algorithm**

I. Introduction

Aiming to provide packet-switched traffic with seamless mobility, high quality of service and minimal latency, handovers play an important role in every cellular communication system. As a recent standard for high data rate communication in telecommunications, the 4th Generation (4G) Long-Term Evolution (LTE) supports two types of handovers including intra-LTE and inter-LTE Mobility Management Entity (MME) handovers [1]–[3]. In the intra-MME handover, i.e. when a User Equipment (UE) moves from a source to a target eNodeB within the same MME, the source eNodeB provides the target eNodeB with a new session key to be used after handover. The session keys are used to encrypt messages, i.e. user data and signaling packets, exchanged between a UE and its serving eNodeB [4]. The new key is generated from the current one by either utilising a one-way function, a.k.a. *backward key separation* process, or adding fresh materials to the process of generating the new one, a.k.a. *forward key separation* process.

As eNodeBs are exposed to the public locations and the internet-protocol-architecture nature of the network, handover-key management process is vulnerable to attacks deployed by bogus eNodeBs [5]. Such attacks are referred to as desynchronisation attacks [6] which aim to prevent target eNodeBs from adding the fresh materials thus breaking the forward key separation process. Consequently, the attacker can either decipher the communications between a genuine eNodeB and a UE or compromise all future keys between specific UEs and eNodeBs for further active attacks. To prevent desynchronisation attacks, the authors of [7] proposed an approach with double authentication. However, both source and destination nodes are required to generate keys, which causes double signaling overhead. Fortunately, the effects of desynchronisation attacks will be terminated at the next update of the root key when handover key materials are generated from scratch instead of deriving from previous keys [8]. In addition to desynchronisation attacks, Denial-of-Service (DoS) attacks, which is beyond the scope of this work, can occur when the UE initiates a detach/attach request during handover to de-register with the old network and re-register with the new one for uninterrupted service.[1] In order to protect against these DoS attacks, an authentication process can be employed for a secure channel between the eNodeB and UE in these phases [10], [11]. The authentication handover and key agreement can be further enhanced with a cross-layer approach over software-defined wireless network [12] where both non-cryptographic and cryptographic information were exploited to cope with latency and security issues.

When an inter-MME handover is carried out for a UE, the root key is automatically updated or regenerated. As a result, all security risks related to the inter-MME handover are eliminated [8]. On the other hand, when an intra-MME handover is performed for the UE, the root key is not updated. In fact, the UE and its serving MME will decide when to regenerate the root key during the residence duration of the UE within that serving MME. Clearly, the intra-MME handovers are vulnerable to desynchronisation attacks. Apart from different approaches for authentication process, see e.g. [10]–[12], the desynchronisation attacks can still occur when

Q.-T. Vien, T. A. Le, and X.-S. Yang are with the Faculty of Science and Technology, Middlesex University, United Kingdom. Email: {q.vien; t.le; x.yang}@mdx.ac.uk.

T. Q. Duong is with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, United Kingdom. Email: trung.q.duong@qub.ac.uk.

[1]A detailed description of the registration and de-registration policies in mobile networks can be referred to in [9].

the root key is not promptly updated in response to the arrival of the UE. Therefore, this paper will focus on tackling the desynchronisation attacks for the intra-MME handovers.

In order to tackle the desynchronisation attacks, in [13], the author first modeled the reliability of typical cryptographic infrastructures, their related failure rates, the failure tolerance of the cryptographic keys, and the accepted error-bound. Then a framework was introduced to maximise the lifetime of the key while bounding the risk of key exposure in the presence of the aforementioned faults. Determining the root Key Update Interval (KUI) has been identified as an effective solution to tackle the desynchronisation attacks, see e.g. [8], [13], [14].[2] To that end, a mathematical model was developed in [8] to represent the average Number of Exposed Packets (NEP) between two root key updates and the average value of Signaling Overhead Rate (SOR).[3] It was shown that the security of intra-MME handovers can be enhanced by minimising the NEP so as to eliminate the desynchronisation attacks. However, such NEP's reduction requires a higher SOR which is undesired and even unfeasible in practice. To address this dilemma, the conventional approaches in [8], [13], [14] aimed to minimise SOR given a required NEP. In this paper, we consider a different approach to simultaneously minimise both the NEP and SOR. To the best of our knowledge, this is the first work addressing the SOR and NEP concurrently where a Multiobjective Optimisation (MO) framework [16], [17] is adopted to capture as well as to find a set of Pareto optimal solutions, i.e. Pareto frontier, for our problem.

Generally, there is no single solution that simultaneously optimises conflicting objectives in an MO problem. However, there exists a set of Pareto optimal solutions, i.e. Pareto frontier [16]. The most suitable/desirable solution to the designer/decision maker is selected from the Pareto frontier. Methods to obtain the Pareto frontier of an MO problem can be mainly classified into two types, i.e. scalarisation approaches and non-scalarisation approaches. In the scalarisation approaches, the preferential information about objectives is known in advance, e.g. defined by the designer/decision maker, an MO problem is then converted into a Single-objective Optimisation (SO) problem by either optimising one objective and considering other objectives as constraints, see e.g. ϵ-constraint method [18], [19], elastic constraint method [20], [21], or aggregating all objectives in a single objective, see e.g. weighted sum method [22], [23], min-max method [24], [25], goal programming [26]–[28], compromise programming [29], [30], and achievement function method (AFM) [31], [32]. On the other hand, in the non-scalarisation approaches, the priority information about objectives is not known in advance. In such case, nature inspired/generic algorithms are usually adopted to generate the Pareto frontier by simultaneously optimising all objectives. The scalarisation approaches attain the Pareto frontier by repeatedly solving several SO problems, each of which is formed with a different value of priorities amongst objectives, while the non-scalarisation approaches obtain the Pareto frontier by directly solving the MO problem. However, the non-scalarisation approaches require significantly higher computational capacity than the scalarisation approaches. Moreover, when the number of objectives increases, the non-scalarisation approaches perform worse than the scalarisation approaches. In this work, we adopt scalarisation approaches to solve our proposed MO problem.

In this paper, we first investigate the impacts of not only KUI but also MME Residence Interval (MRI) on the handover performance in terms of NEP and SOR. In order to evaluate the secrecy performance of the handover mechanism, we also analyse the Outage Probability of Vulnerability (OPV) which is defined as the probability that the handover is at-risk caused by desynchronisation attacks.[4] The derived OPV as well as the bounds of the NEP and SOR facilitate the finding of the optimal KUI and MRI to minimise both the NEP and SOR using various approaches. The main contributions of this paper can be summarised as follows:

- Upper and lower bounds of NEP and SOR are derived with respect to KUI and MRI. The derived bounds provide insightful meanings of the NEP and SOR expressions. They not only capture the behaviours of the NEP and SOR at the boundary values of the KUI and MRI, but also verify that there exists a trade-off between the NEP and the SOR.
- The OPV is derived as a function of both the KUI and MRI given a vulnerable period threshold. It is shown that the OPV monotonically increases as either the KUI or the MRI increases. This accordingly indicates that the desynchronisation attacks can be eliminated when the MRI lasts for a short time; otherwise, the OPV can be reduced by shortening the KUI to enhance the handover security.
- An MO problem is proposed to find the optimal KUI and MRI that minimise both the NEP and SOR subject to the constraint on the OPV. Observing the properties of the derived bounds on NEP and SOR motivates us to adopt an achievement function method [16, Definition 4.28] to scalarise the proposed MO problem, i.e. transforming the proposed MO problem into an SO problem, as the ratio of the normalised NEP to the normalised SOR. In fact, the transformed SO problem is also a Fractional Programming (FP) problem. Thanks to the derived bounds of the NEP and SOR, the FP problem can be solved via a simple numerical method, which hereafter is referred to as the boundary-based FP. The boundary-based FP can avoid the conventional exhaustive search of the KUI, e.g. in [8], which in turn reflects the novelty of our work in deriving the aforementioned bounds. Hence, adopting our proposed boundary-based FP approach instead of utilising the standard method in [8] to tackle desynchronisation

[2]An overview of various kinds of attacks in mobile networks can be referred to in [15] where desynchronisation attack is the one against handover key management and the selection of an optimal root KUI is shown to be an approach to mitigate the effect of such attack.

[3]The SOR is defined as the number of bits for individual authentication among the UEs, the MME and the home subscriber server/authentication centre during intra-MME handovers.

[4]This work is extended from [33] where only the impacts of the KUI and MRI were considered on the optimisation of handover security performance. We now take a further step with the analysis of the OPV and the proposal of two approaches for solving the developed MO problem.

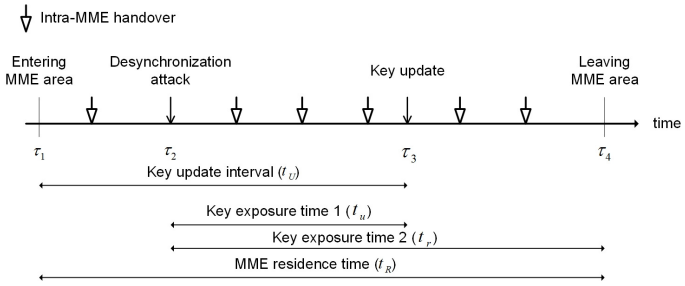


Fig. 1: Timing diagram of MME residence with key update and vulnerable attack periods [8].

attacks in intra-MME handovers[5] results in not only a reduced complexity but also an improved reliability. Furthermore, given a constraint on the maximal OPV, the maximum values of the KUI and MRI can be obtained, which are helpful in verifying the appropriateness of the derived optimal KUI and MRI.

- As a metaheuristic approach, Firefly Algorithm (FA) is adopted as a second approach to solve another scalarised version of the proposed MO problem which is a weighted sum of the normalised NEP and SOR, hereafter it is referred to as the FA approach. The FA approach is shown to provide a quick convergence of the fireflies towards the optimal values after a small number of generations, and thus promising to provide a self-adjusting and adaptive MME handover.

The rest of this paper is organised as follows: Section II describes the system model of a typical MME handover in LTE networks. The bounds of NEP and SOR with respect to KUI and MRI are derived in Section III, followed by the analysis of OPV in Section IV. Sections V and VI sequentially present FP and FA methods for optimising the KUI and MRI. Numerical and simulation results are presented in Section VII to validate the concepts and findings. Finally, Section VIII draws the main conclusions from this paper.

II. System Model

Figure 1 illustrates the timing diagram of an MME residence in a typical LTE network [8]. Consider the following times in a chronological order τ_1, τ_2, τ_3 and τ_4. A UE enters an MME area at τ_1 and leaves at τ_4. An intra-MME handover over X2 interface between eNodeBs is investigated, while the signalling of UE association between eNodeB and the MME is offered via S1 interface [34].[6] When an intra-MME handover is occurred, a new session key is generated by applying a one-way function to the current session key. In order to prevent irrelevant eNodeBs from deriving a new session key from the current session key, i.e., maintaining the forward-key-separation process, fresh materials are added to the process of creating the key. However, under certain circumstances, handover key management cannot guarantee the forward-key-separation process against variant attacks by bogus eNodeBs [8], a.k.a. desynchronisation attacks. Fortunately, the desynchronisation attack will be terminated when the root key is updated.

In Fig. 1, a desynchronisation attack and a root key update requested by the UE are assumed to take place at τ_2 and τ_3, respectively.[7] As a part of handover preparation, the UE performs measurements of the received signals from the neighboring eNodeBs and sends the measurement reports to the source eNodeB to identify the target cell(s) for handover [36]. During this phase, the uplink and downlink channels for LTE Radio Resource Control (RRC) connection establishment procedure are secured for sharing the measurement reports between the UE and eNodeB, controlling the key sharing, signalling of handover requests, and acknowledgement between eNodeBs.

Let us denote the MRI and KUI by t_R and t_U, respectively. As shown in Fig. 1, $t_R = \tau_4 - \tau_1$ and $t_U = \tau_3 - \tau_1$. Furthermore, let $t_u = \tau_3 - \tau_2$ and $t_r = \tau_4 - \tau_2$ denote two key exposure intervals with reference to the key update time and the MME exiting time, respectively. The effect of a desynchronisation attack can be eliminated at the time when either updating key or the UE leaves the MME. It is therefore crucial to determine the optimal KUI and MRI to alleviate the desynchronisation attacks. The vulnerable period, denoted by t_c, is accordingly determined by

$$t_c = \min\{t_u, t_r\}. \tag{1}$$

Note that if the desynchronisation attack occurs after the key is updated, i.e. $\tau_3 \leq \tau_2$, then there is only the second key exposure interval as regards the MME exiting time, and thus $t_c = t_r$.

In order to model the interval time of key update, following the same approach as in [8], let us assume that KUI, i.e. t_U, follows an exponential distribution [37] with a rate of μ_u.[8] For modelling variant duration and mobility of UEs in various environment, the MRI, i.e. t_R, is assumed to follow a gamma distribution [38] which is a general type of statistical distribution with a shape parameter of k and a rate of μ_r.[9] Here, μ_u and μ_r represent the key update rate and mobility rate of UEs, respectively. The average KUI, denoted by T_U,

[5]Our solution is not required for standard inter-MME handover since the root key is automatically updated or regenerated during this process.

[6]Details of mechanism considered for intra-handover over X2 interface can be referred to in [34] where X2 Application Protocol (X2AP) was introduced for the handover process between eNodeBs. Specifically, the mobility management in the X2AP between the master eNodeB (MeNB) and the secondary eNodeB (SeNB) consists of the following elementary procedures: *Handover preparation*, *Sequence number status transfer*, *UE context release*, and *Handover cancel*.

[7]Depending the capacity of the eNodeB, the handover of multiple UEs can be executed simultaneously by grouping them together via group handover as in [35]. In this work, we considered an intra-MME handover of an UE with a desynchronisation attack. The work however can be extended for the case of multiple UE handovers where the desynchronisation attacks at different UEs can be treated individually by utilising different KUIs correspondingly.

[8]Exponential distribution is used to model the KUI due to its memoryless property in describing the time interval between events which occur independently with a constant rate [37], [38].

[9]Gamma distribution has been shown to be a good approximation for the cell residence time distribution considering user mobility in cellular networks [39].

TABLE I: Summary of main notations

Notation	Meaning
τ_i, $i = 1, 2, 3, 4$	UE arrival time, attack time, key update time and UE departure time, respectively
t_R and t_U	MME residence interval (MRI) and key update interval (KUI), respectively
t_r and t_u	key exposure intervals with reference to key update time and MME departure time, respectively
t_c	vulnerable period
T_R and T_U	average MRI and average KUI, respectively
k and μ_r	shape parameter and rate of gamma distribution representing MRI
μ_u	rate of exponential distribution representing KUI
$E[\cdot]$	expectation operator
N and S	number of exposed packets (NEP) and signalling overhead rate (SOR), respectively
λ_p	average arrival rate of packets exchanged between UE and eNodeB
ρ	number of bits for authentication
P_o	outage probability of vulnerability (OPV)
τ_{th}	vulnerable interval threshold
$F_X[\cdot]$	cumulative distribution function (cdf) of a random variable X
$\Gamma(z)$ and $\Gamma(a, z)$	gamma function and upper incomplete gamma function, respectively
α	required maximum OPV
$\nu(x)$	ratio of the normalised NEP to the normalised SOR
δ	relative important factor
w_1 and w_2	weighting factors
$I(x, y)$	light intensity of a firefly at (x, y)
I_0	original light intensity of source
γ	light absorption coefficient
$\beta_{i,j}$	attractiveness of a firefly i with respect to a firefly j with distance $r_{i,j}$
ϕ	randomisation parameter
N_F and $G_{\max}$	number of fireflies and maximum generation, respectively

and the average MRI, denoted by T_R, are thus given by [37], [38]

$$T_U \triangleq E[t_U] = \frac{1}{\mu_u}, \tag{2}$$

$$T_R \triangleq E[t_R] = \frac{k}{\mu_r}, \tag{3}$$

where $E[\cdot]$ denotes the expectation operator.

Remark 1 (*The appropriateness of gamma distribution for modelling MRI*)**.** *It can be noticed in* (3) *that $T_R \to \infty$ if $\mu_r \to 0$ and $T_R \to 0$ if $\mu_r \to \infty$. This accordingly means that there is no handover when the UEs are immobile, while the MRI is very short in case that the UEs move very fast. A further notice is that the gamma distribution is skewed by $2/\sqrt{k}$ [40] depending on the shape parameter, and thus can be exploited to reflect the asymmetry of the mobility of the UEs. For example, as illustrated in [39], $k = 2.31$ for the UE with an average speed of 50 km/h. These facts indeed verify that the gamma distribution is an appropriate modelling for the MRI.*

In this work, we aim to find the optimal MRI and KUI, i.e. to decide optimal times to regenerate the root key, to tackle desynchronisation attacks. Key sharing mechanisms are out of the scope of our work. For convenience, the main notations used in the paper are listed in Table I.

III. Bounds of NEP and SOR

During the vulnerable period, i.e. t_c, user data and signaling packets exchanged between the UE and eNodeB are exposed to eavesdroppers. An approach to mitigate desynchronisation attacks during an MME handover is to minimise the number of exposed packets (NEP) between two root key updates. However, such reduced NEP is achieved at a cost of higher signaling overhead rate (SOR) in terms of the number of bits for authentication. In this section, the NEP and SOR are first analysed to show their impacts on the security of the MME handover. Their contradictory behaviours are then deduced, which leads to the development of optimisation problems in Sections V and VI. The average NEP, i.e. $E[N]$, and the average SOR, i.e. $E[S]$, can be expressed as in [8], i.e.

$$E[N] = \frac{\lambda_p}{\mu_u}\left(1 - \frac{\mu_r}{\mu_u k}\left(1 - \left(\frac{\mu_r}{\mu_u + \mu_r}\right)^k\right)\right), \tag{4}$$

$$E[S] = \frac{\rho}{\frac{1}{\mu_u} + \frac{k}{\mu_r}}, \tag{5}$$

where λ_p is the mean arrival rate of packets exchanged between the UE and eNodeB; and ρ is the number of bits in the messages for individual authentication among the UEs, the MME and the home subscriber server/authentication centre.

In order to provide the insightful meanings of the above expressions, let us derive the limits of the average NEP and SOR as the average root KUI T_U and MRI T_R approach 0 and ∞. The findings are presented in the following three lemmas:

Lemma 1. *The average NEP, i.e. $E[N]$, is an increasing function of $T_U \in (0, \infty)$, which is lower bounded by $N_{\min}^{(T_U)} = 0$ and upper bounded by*

$$N_{\max}^{(T_U)} = \frac{\lambda_p(k+1)}{2\mu_r}. \tag{6}$$

Proof. See Appendix A. □

Lemma 2. *The average NEP, i.e. $E[N]$, is an increasing function of $T_R \in (0, \infty)$, which is upper bounded by*

$$N_{\max}^{(T_R)} = \frac{\lambda_p}{\mu_u}, \tag{7}$$

while it is lower bounded by

$$N_{\min}^{(T_R)} = \frac{\lambda_p}{\mu_u}\left(1 + \frac{\mu_r}{\mu_u}\log\left(\frac{\mu_r}{\mu_u + \mu_r}\right)\right) \tag{8}$$

when $k \to 0$ and $N_{\min}^{(T_R)} = 0$ when $\mu_r \to \infty$.

Proof. See Appendix B. □

Lemma 3. *The average SOR, i.e. $E[S]$, is a decreasing function of both $T_U \in (0, \infty)$ and $T_R \in (0, \infty)$, in which both are lower bounded by 0, while they are upper bounded by*

$$S_{\max}^{(T_U)} = \frac{\rho\mu_r}{k} = \frac{\rho}{T_R}, \tag{9}$$

$$S_{\max}^{(T_R)} = \rho\mu_u = \frac{\rho}{T_U}. \tag{10}$$

Proof. From (5), it can be shown that $E[S]$ decreases as either $T_U = 1/\mu_u$ or $T_R = k/\mu_r$ increases. Also, $E[S] \to 0$ when either $T_U \to \infty$ or $T_R \to \infty$, and thus it is lower bounded by 0. When $T_U \to 0$, i.e. $\mu_u \to \infty$, we obtain the upper bound of $E[S]$ as

$$S_{\max}^{(T_U)} = \lim_{\mu_u \to \infty} E[S] = \frac{\rho}{\frac{k}{\mu_r}} = \frac{\rho}{T_R}. \tag{11}$$

Similarly, when $T_R \to 0$, i.e. $\mu_r/k \to \infty$, $E[S]$ is upper bounded by

$$S_{\max}^{(T_R)} = \lim_{\mu_r/k \to \infty} E[S] = \frac{\rho}{\frac{1}{\mu_u}} = \frac{\rho}{T_U}. \tag{12}$$

This completes the proof. □

Lemmas 1, 2 and 3 indicate that reducing either the KUI or MRI lowers the risk of security breaches, i.e. reducing NEPs, at the cost of an increase in signaling overhead. Hence, minimising the average NEP over either T_U or T_R is contradicting with minimising the average SOR. In Section V, we introduce a method to find optimal values of T_U and T_R in order to balance between the two conflicting objectives.

IV. Analysis of Outage Probability of Vulnerability

Apart from analysing NEP and SOR as in Section III, it is critical to investigate the security of MME handover. This section analyses the OPV of the key update and MME residence management processes. Here, the OPV is defined as the probability that the handover is harmed by desynchronisation attacks, i.e. when the vulnerable period of the handover is longer than a threshold value. Letting P_o denote the OPV of the handover process, we have

$$P_o \triangleq \Pr\{t_c > \tau_{th}\}, \tag{13}$$

where t_c is a vulnerable period and τ_{th} is a vulnerable interval threshold.[10]

As described in Section II, $t_c = \min\{t_u, t_r\}$, where $t_u = \tau_3 - \tau_2$, $t_r = \tau_4 - \tau_2$. The OPV in (13) can be computed by

$$\begin{aligned} P_o &= \Pr\{\min\{t_u, t_r\} > \tau_{th}\} \\ &= \Pr\{\min\{\tau_3 - \tau_2, \tau_4 - \tau_2\} > \tau_{th}\} \end{aligned} \tag{14}$$

Note that the KUI, i.e. t_U, and MRI, i.e. t_R, are given by $t_U = \tau_3 - \tau_1$ and $t_R = \tau_4 - \tau_1$. Therefore, t_c can also be determined by $\min\{t_U, t_R\}$ and (14) can be rewritten using order statistics as

$$\begin{aligned} P_o &= \Pr\{\min\{t_U, t_R\} > \tau_{th}\} \\ &= \Pr\{t_U > \tau_{th}\} \Pr\{t_R > \tau_{th}\} \\ &= \left(1 - F_{t_U}(\tau_{th})\right) \left(1 - F_{t_R}(\tau_{th})\right), \end{aligned} \tag{15}$$

where $F_X[\cdot]$, $X \in \{t_U, t_R\}$, denotes the cumulative distribution function (cdf) of a random variable X. We have the following finding:

[10]The vulnerable interval threshold τ_{th} is set according to the practical handover requirement in different network models to maintain its security against desynchronisation attacks. For example, a small τ_{th} should be considered for a dense network where desynchronisation attacks are likely to occur.

Lemma 4. *The OPV of MME handover is determined by*

$$P_o = \frac{\Gamma(k, \mu_r \tau_{th})}{\Gamma(k)} e^{-\mu_u \tau_{th}}, \tag{16}$$

where $\Gamma(z) \triangleq \int_0^\infty e^{-t} t^{z-1} dt$, $\Re\{z\} > 0$, *is the gamma function [41, eq. (8.310.1)] and* $\Gamma(\alpha, z) \triangleq \int_z^\infty e^{-t} t^{\alpha-1} dt$ *is the upper incomplete gamma function [41, eq. (8.350.2)].*

Proof. See Appendix C. □

Corollary 1. *Given k is a positive integer, the OPV can be obtained by*

$$P_o = e^{-(\mu_u + \mu_r)\tau_{th}} \sum_{i=0}^{k-1} \frac{(\mu_r \tau_{th})^i}{i!}. \tag{17}$$

Proof. When k is a positive integer, the gamma function and upper incomplete gamma function in (16) can be computed by [41, eq. (8.339.1) & eq. (8.352.2)], i.e.

$$\Gamma(k) = (k-1)!, \tag{18}$$

$$\Gamma(k, \mu_r \tau_{th}) = (k-1)! e^{-\mu_r \tau_{th}} \sum_{i=0}^{k-1} \frac{(\mu_r \tau_{th})^i}{i!}. \tag{19}$$

Substituting (18) and (19) into (16), we obtain (17). □

Remark 2 (*A lower OPV with either a lower KUI or a lower MRI*)**.** *In fact, from* (17)*, it can be easily shown that P_o monotonically decreases as either μ_u or μ_r increases. Since $T_U = 1/\mu_u$ and $T_R = k/\mu_r$, we can deduce that P_o increases over T_U and T_R. This accordingly means that a short MRI results in a lower OPV and the desynchronisation attacks can also be eliminated by shortening the KUI. In other words, a more secure handover can be obtained with either a high-mobility user or a fast key update.*

V. Boundary-Based Fractional Programming for Optimising KUI & MRI

As shown in Sections III and IV, the average NEP, i.e. $E[N]$, and OPV, i.e. P_o, increase while the average SOR, i.e. $E[S]$, decreases as either the KUI, i.e. T_U, or the MRI, i.e. T_R, increases (see Lemmas 1, 2, 3 and 4). In other words, either a short and frequent KUI or a short MRI causes a waste of signalling overhead, but helps reduce the risk of security breaches with small NEP and OPV. This essentially becomes a constrained optimisation problem of finding optimal values of T_U and T_R in order to balance between the NEP and the SOR subject to the constraint of the OPV.[11]

We first bring the average NEP and SOR into the same scale by defining the following normalised functions

$$N(x) \triangleq \frac{E[N]}{N_{\max}^{(x)}}, \tag{20}$$

$$S(x) \triangleq \frac{E[S]}{S_{\max}^{(x)}}, \tag{21}$$

[11]The optimisation also holds for the key update rate μ_u since T_U is inversely proportional to μ_u (see (2)).

where $x \in \{T_U, T_R\}$; $E[N]$ and $E[S]$ are given by (4) and (5), respectively; and $N_{\max}^{(T_U)}$, $S_{\max}^{(T_U)}$, $N_{\max}^{(T_R)}$ and $S_{\max}^{(T_R)}$ are derived in Section III by (6), (9), (7) and (10), respectively. We can thus rewrite (20) and (21) as (22) (on the top of next page) and

$$S(x) = \begin{cases} \dfrac{T_R}{x + T_R} & \text{if } x = T_U, \\ \dfrac{T_U}{x + T_U} & \text{if } x = T_R, \end{cases} \tag{23}$$

respectively.

Finding an optimal x that minimises both functions $S(x)$ and $N(x)$ is actually solving the following bi-objective optimisation problem [16]:

$$\min_{x \in [0,\infty)} \{S(x), N(x)\} \tag{24}$$

s. t.

$$P_o(x) \leq \alpha, \tag{25}$$

where α denotes the required maximum OPV to guarantee the handover security and $P_o(x)$, $x \in \{T_U, T_R\}$, is given by (16) in Lemma 4. Note that optimising the KUI and MRI are two separate optimisation problems of T_U and T_R, respectively. Here, for brevity, we have grouped these two problems into one as shown in (24) when $x = T_U$ or $x = T_R$. Specifically, considering the scenario that the shape parameter of the gamma distribution of the MRI, i.e. k, is a positive integer number, $P_o(x)$ can be determined using Corollary 1 as follows

$$P_o(x) = \begin{cases} e^{-(1/x+\mu_r)\tau_{th}} \sum_{i=0}^{k-1} \dfrac{(\mu_r \tau_{th})^i}{i!} & \text{if } x = T_U, \\ e^{-(\mu_u + k/x)\tau_{th}} \sum_{i=0}^{k-1} \dfrac{(k\tau_{th}/x)^i}{i!} & \text{if } x = T_R. \end{cases} \tag{26}$$

From Lemmas 1, 2 and 3, it can be verified that $S(x)$ and $N(x)$ are also decreasing and increasing functions, respectively, with respect to x. Those properties stimulate us to scalarise the proposed MO problem (24) by forming an achievement function [16, Definition 4.28] $\nu(x) \triangleq \dfrac{N(x)}{S(x)}$ as the ratio of the normalised NEP to the normalised SOR. It will be shown latter in this section that adopting the achievement-function method leads to a simple numerical approach using the derived bounds of the NEP and SOR. From (22) and (23), $\nu(x)$ can be written by (27) (on the top of next page).

Furthermore, let us denote δ as the relative importance factor determined by the network operator as the ratio of the average NEP to SOR.[12] The MO problem in (24) can be transformed into the following SO problem to find the optimal solution x while balancing the two conflicting objectives and satisfying the OPV constraint (see (25)).

$$\min_{x \in (0,\infty)} x \tag{28}$$

s. t.

$$\nu(x) \geq \delta, \tag{29}$$

[12]Lowering the signaling overheads beyond a certain point increases the risk of other attacks on the network entities. By varying the important factor δ, the Pareto frontier for the proposed MO problem can be attained. Hence, the operator/decision maker can select a suitable operation point from the Pareto frontier satisfying the required value of signaling overhead.

$$P_o(x) \leq \alpha. \tag{30}$$

In fact, problem (28) is also a FP. According to [16, Theorem 4.29], the optimal solution to the FP (28) is also the optimal solution to the original MO problem (24). Solving the above optimisation problem, we have the following boundary-based FP problem:

Lemma 5 (*FP Method*)**.** *The optimal T_U and T_R can be obtained as follows*

$$x_{opt} = x | \nu(x) = \delta \wedge x \leq x_{\max}, \tag{31}$$

where $x \in \{T_U, T_R\}$ and $x_{\max}$ is found by solving $P_o(x) = \alpha$.

Proof. It can be shown that $\nu(x)$, $x \in \{T_U, T_R\}$, is an increasing function with respect to x since $S(x)$ and $N(x)$ are decreasing and increasing functions, respectively, over x. The optimal solution to (28), i.e. x_{opt}, can be thus obtained by solving the equation $\nu(x) = \delta$ where $\nu(x)$ is given by (27). Additionally, as noted in Remark 2, the OPV increases as either the KUI or the MRI increases, i.e. $P_o(x)$ increases over x. Therefore, given the constraint (30) on the required maximum OPV, we can determine the maximum value of x, i.e. $x_{\max}$, by solving $P_o(x) = \alpha$ where $P_o(x)$ is given by (26). This accordingly means that in order to guarantee the OPV requirement, the optimal values of the KUI and MRI should also not exceed these maximum values. The Lemma is proved. □

Corollary 2. *The optimal value x_{opt} in* (31) *can be found only when $0 < \delta \leq \delta_{\max}$, where $\delta_{\max} = \nu(x_{\max})$ and $P_o(x_{\max}) = \alpha$.*

Proof. The proof can be straightforwardly obtained with the notice from Lemma 5 that $\nu(x)$ monotonically increases over x and with the constraint $x \leq x_{\max}$. □

Remark 3 (*Impacts of relative important factor between NEP and SOR*)**.** *It can be noticed that, if $\delta \to 0$, then solving* (31)*, i.e. $\nu(x) \to 0$, means $N(x) \to 0$ and $S(x) \to 1$. Similarly, if $\delta \to \infty$, then we need to solve $\nu(x) \to \infty$, i.e. $S(x) \to 0$ and $N(x) \to 1$. Furthermore, from Corollary 2, the relative important factor should be restricted in a specific range, i.e. $\delta \in (0, \delta_{\max}]$, which can be determined through the OPV constraint.*

For clarity, the finding of the optimal KUI and MRI with the proposed boundary-based FP is summarised in Algorithm 1.

In order to examine the practicality of the proposed FP algorithm, let us consider the following example:

Example 1. *A UE experiences intra-MME handover with the following parameters: the mean packet arrival rate $\lambda_p = 64$ kbits/s, the number of bits in authentication message $\rho = 1$ kbits, the relative importance factor $\delta = 0.3$, the required maximum OPV $\alpha = 0.01$, the vulnerable interval threshold $\tau_{th} = 5$ seconds and the shape parameter $k = 1$. By employing Algorithm 1, it can be arrived at $T_U = 1.8$ seconds when $T_R = 6$ seconds, while $T_U = 2.5$ seconds when $T_R = 8$*

$$N(x) = \begin{cases} \dfrac{2kx}{(k+1)T_R}\left(1 - \dfrac{x}{T_R}\left(1 - \left(\dfrac{kx}{kx+T_R}\right)^k\right)\right) & \text{if } x = T_U, \\ 1 - \dfrac{T_U}{x}\left(1 - \left(\dfrac{kT_U}{x+kT_U}\right)^k\right) & \text{if } x = T_R, \end{cases} \tag{22}$$

$$\nu(x) = \begin{cases} \dfrac{2kx(x+T_R)}{(k+1)T_R^2}\left(1 - \dfrac{x}{T_R}\left(1 - \left(\dfrac{kx}{kx+T_R}\right)^k\right)\right) & \text{if } x = T_U, \\ \dfrac{x+T_U}{T_U}\left(1 - \dfrac{T_U}{x}\left(1 - \left(\dfrac{kT_U}{x+kT_U}\right)^k\right)\right) & \text{if } x = T_R. \end{cases} \tag{27}$$

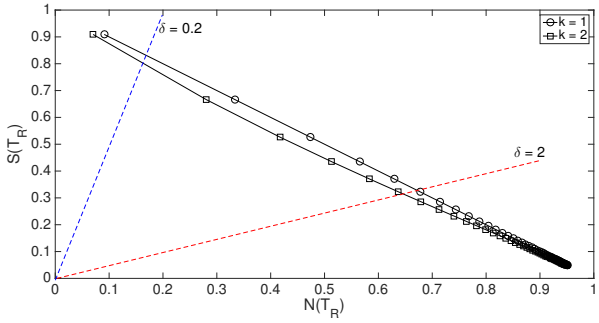
Algorithm 1 (Fractional Programming Algorithm)

Input: k, τ_{th}, α and $\delta \in (0, \delta_{\max}]$ (see Corollary 2)
Find $x \in \{T_U, T_R\}$: $\nu(x) = N(x)/S(x) = \delta$
    where $\nu(x)$ is given by (27)
Determine $x_{\max}$: $P_o(x_{\max}) = \alpha$ (see Lemma 5)
    where $P_o(x)$, $x \in \{T_U, T_R\}$, is given by (26)
if $x \le x_{\max}$ **then**
    $x_{opt} = x$
else
    $x_{opt} = x_{\max}$
end if
Output: $T_{U,opt}$, $T_{R,opt}$

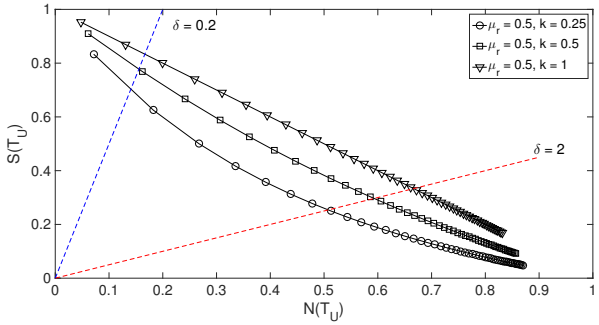
seconds. This accordingly means that, in order to mitigate desynchronisation attacks, the KUI should be less than 1.8 seconds and 2.4 seconds when the duration that the UE stays within an MME, i.e. MRI, is 6 seconds and 8 seconds, respectively.

A graphical illustration of the relationship between the normalised NEP and the normalised SOR is shown in Fig. 2. In Fig. 2(a), $S(T_R)$ is plotted versus $N(T_R)$, while $S(T_U)$ is plotted versus $N(T_U)$ in Fig. 2(b) with respect to various μ_r and k. As stated in Lemma 5, for every value of δ, the optimal values of T_R and T_U are the crossing points between the line $S(x) = N(x)/\delta$ and the curve $S(N(T_R))$ and $S(N(T_U))$ in Figs. 2(a) and 2(b), respectively. Also, these illustrations verify the notice in Remark 3 as δ approaches either 0 or ∞.

Remark 4 (*Reduced complexity via FP approach*)**.** *It can be observed that, by deriving the bounds of the average NEP and the average SOR in Section III, the optimisation problem in* (28) *can be easily solved by a numerical method. Specifically, the proposed FP approach can provide optimal KUI and MRI by solving two equations, as stated in Lemma 5, rather than performing exhaustive searches as in the conventional approach, e.g. [8]. This not only helps reduce the complexity in finding the optimal solutions, but also improves the reliability with numerical approach, which accordingly reflects the novelty of our work in finding the bounds for the NEP and SOR in Section III.*



(a)



(b)

Fig. 2: (a) $S(T_R)$ versus $N(T_R)$ with $T_U = 3$ seconds; (b) $S(T_U)$ versus $N(T_U)$ with $\rho = 1$ kbits and $\lambda_p = 64$ kbits/s.

VI. Firefly Algorithm for Optimising KUI & MRI

In this section, we adopt a popular weighted-sum method to scalarise the MO problem into an SO problem. To that end, the scalarised version of the MO problem (24) can be formulated as the following SO problem:

$$\min_{T_U, T_R} f(T_U, T_R) = w_1 N(T_U, T_R) + w_2 S(T_U, T_R) \tag{30}$$

s. t.

$$P_o(T_U, T_R) \le \alpha, \tag{31}$$

where w_1 and w_2 are weighting factors satisfying $w_1 + w_2 =$

1.[13] For convenience, let us denote the value set of (T_U, T_R) by (x, y) which can be regarded as spatial coordinates of a point in 2D. From (22), (23) and (26) with a notice that $\mu_r = k/T_R$, we can rewrite the objective (30) and constraint (31) by replacing $x = T_U$ and $y = T_R$ as follows:

$$\min_{x,y} f(x,y) = \left\{ w_1 \left[1 - \frac{x}{y} \left(1 - \left(\frac{kx}{kx+y} \right)^k \right) \right] + w_2 \frac{x}{x+y} \right\} \tag{32}$$

s. t.

$$e^{-(1/x+k/y)\tau_{th}} \sum_{i=0}^{k-1} \frac{(k\tau_{th})^i}{y^i i!} \leq \alpha \tag{33}$$

According to [16, Theorem 3.11], the optimal solution to the SO problem (32) is also the optimal solution to the MO problem (24). Given preferential information of w_1 and w_2, it is very challenging to derive a numerical method to solve the above SO problem (32). Fortunately, nature-inspired metaheuristic algorithms can be exploited to obtain the optimal solution. Specifically, FA has recently emerged as one of the powerful biologically inspired algorithms to solve various optimisation problems [42] by offering more naturally and efficiently environmental awareness in decision making and learning processes. Although there are various evolutionary algorithms to deal with diverse optimisation problems [43], such as genetic algorithm [44], [45], ant colony optimisation algorithm [46], [47], particle swarm optimisation algorithm [48], [49], etc., the FA is shown to be more natural and efficient compared to the other counterparts [42]. It is noted that FA has been proposed to cope with the MO problems in various applications, for instance, pressure vessel design [50], flowshop scheduling problems [51], economic emissions load dispatch problems [52], structural optimisation [53] and telecommunications [54]. Due to the above facts, the FA is exploited in this work to solve the proposed problem (32). In the following, the FA is briefly introduced, followed by its adaptation for the MO problem under investigation.

A. Firefly Algorithm (FA)

Fireflies, a.k.a. lightning bugs, produce short and rhythmic flashing lights to not only attract mating partners and potential preys, but also help in defensive vigilance. With about 2000 species of fireflies, the pattern of their flashes is unique for different species with different flashing rate and duration. By observing the fundamental functions of the flashes and their light intensity at various distances, the flashing light can be formulated to model the objective function which can be solved with FA.

In order to describe the FA, for simplicity, the flashing characteristics of fireflies are firstly idealised as follows [42]:

i) All the fireflies are unisex and thus can attract each other irrespective of their sex;
ii) Attractiveness of the fireflies is proportional to their brightness, while inversely proportional to the distance between them;
iii) The brightness of a firefly is affected by the topography of the objective function. For a maximisation problem, the brightness is simply proportional to the objective function value, while for a minimisation problem, the brightness can be represented by the reciprocal of the objective function value.

It is noted that the light intensity received at a specific node of distance r with respect to a light source varies as

$$I(r) = I_0 e^{-\gamma r^2}, \tag{34}$$

where I_0 is the original light intensity of the source and γ is the light absorption coefficient which is dependent on the transmission medium assumed to be fixed. According to the second rule of the FA, the attractiveness of a firefly i with respect to a firefly j can be similarly formulated as follows

$$\beta_{i,j} = \beta_0 e^{-\gamma r_{i,j}^2}, \tag{35}$$

where β_0 is the attractiveness at $r_{ij} = 0$ and the distance between a firefly i at (x_i, y_i) and a firefly j at (x_j, y_j) is determined by the Euclidean distance as

$$r_{i,j} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}. \tag{36}$$

Additionally, the random movement of a firefly j towards a more attractive firefly i is modeled as [42]

$$x_j = x_j + \beta_{i,j}(x_i - x_j) + \varphi \left(U_x - \frac{1}{2} \right), \tag{37}$$

$$y_j = y_j + \beta_{i,j}(y_i - y_j) + \varphi \left(U_y - \frac{1}{2} \right), \tag{38}$$

where U_x and U_y are uniformly distributed random numbers in the interval $(0, 1)$ and φ is randomisation parameter which is assumed to vary in $(0, 1]$.

B. Optimising KUI & MRI with FA

Adopting the FA approach in solving the MO problem in (32), the light intensity of a firefly at (x, y) is represented by the reciprocal of the objective function,[14] i.e.

$$I(x,y) = \left\{ w_1 \left[1 - \frac{x}{y} \left(1 - \left(\frac{kx}{kx+y} \right)^k \right) \right] + w_2 \frac{x}{x+y} \right\}^{-1} \tag{39}$$

Let N_F and $G_{\max}$ denote the number of fireflies and their maximum generation, respectively. The FA approach for finding the optimal KUI and MRI subject to the constraint on the OPV is carried out as in Algorithm 2.

[13] By varying the weighting factors w_1 and w_2, the Pareto frontier for the proposed MO problem can be attained. From the Pareto frontier, the operator/decision maker can select a suitable operation point satisfying the required value of signaling overhead to eliminate the risk of other attacks on the network entities.

[14] The reciprocity of light intensity and objective function is stated in the third rule of FA in previous subsection when the considered optimisation problem is a minimisation problem.

Algorithm 2 (Firefly Algorithm)

Input: $G_{\max}$, N_F, ϕ, γ, α, τ_{th}, k, w_1, w_2
Generate initial population ($g = 1$) of N_F fireflies $\{(x_1, y_1), (x_2, y_2), \ldots, (x_{N_F}, y_{N_F})\}$ satisfying $\{P_o(x, y) \leq \alpha\}$ (see (33))
Determine the light intensity at all fireflies $\{I_i(x_i, y_i)\}$, $i = 1, 2, \ldots, N_F$, using (39)
repeat
  for $i = 1$ **to** N_F **do**
    for $j = i + 1$ **to** N_F **do**
      if $I_j > I_i$ **then**
        Move firefly i towards firefly j with new position (x_i', y_i') (see (37) and (38))
        if $P_o(x_i', y_i') \leq \alpha$ **then**
          Update attractiveness between fireflies (see (35))
          Update light intensity at fireflies w.r.t. new position
          $x_{opt} = x_i'$, $y_{opt} = y_i'$
        else
          Move firefly i back to the original position
        end if
      end if
    end for
  end for
  Rank all fireflies in ascending order of their light intensity
  $g \leftarrow g + 1$
until ($g \leq G_{\max}$)
Output: $T_{U,opt} = x_{opt}$ $T_{R,opt} = y_{opt}$

TABLE II: Simulation parameters

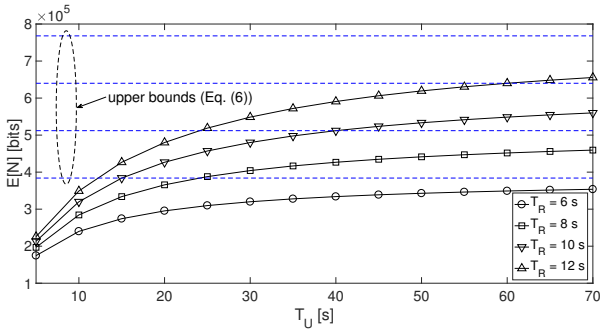
Parameter	Value(s)
λ_p	64 kbits/s
ρ	1000 bits
μ_r	$\{1/6, 1/8, 1/10, 1/12\}$ [sec^{-1}] with $k = 1$
μ_u	$\{1/2, 1/4, 1/6, 1/8\}$ [sec^{-1}]
α	$\{0.01, 0.001\}$
τ_{th}	$\{0 : 20\}$ [sec]
N_F	20
G_{max}	50
ϕ	0.3
γ	1

VII. Numerical Results

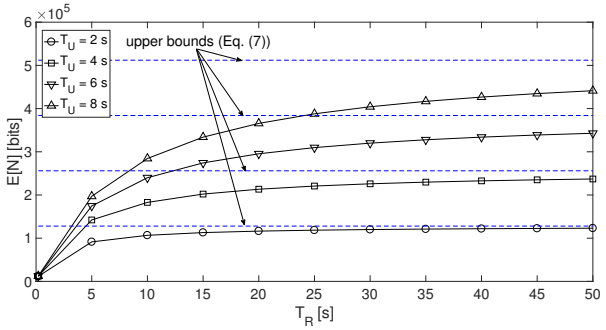
In this section, we first present numerical results of three performance metrics, including NEP, SOR and OPV, followed by the optimisation of the KUI and MRI for the handover security key management using FP and FA approaches. The values of typical parameters used in the numerical evaluations are provided in Table II unless otherwise stated.

A. The impacts of KUI and MRI on NEP Performance

Figures 3(a) and 3(b) sequentially plot the average NEP, i.e. $E[N]$ [bits], as a function of KUI, i.e. T_U [s], and MRI, i.e. T_R [s], respectively. It is assumed that the mean arrival rate of packets exchanged between the UE and eNodeB is $\lambda_p = 64$ kbits/s. In Fig. 3(a), various scenarios of $T_R \in \{6, 8, 10, 12\}$



(a)



(b)

Fig. 3: (a) $E[N]$ versus T_U w.r.t. T_R; (b) $E[N]$ versus T_R w.r.t. T_U.

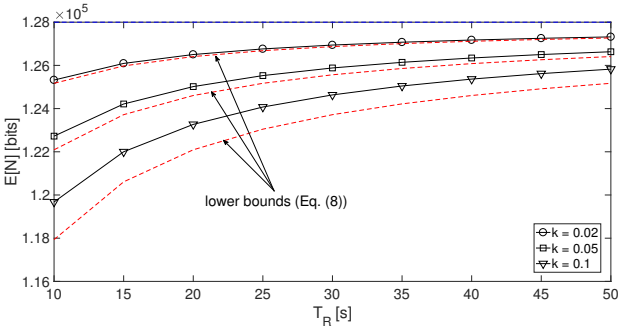
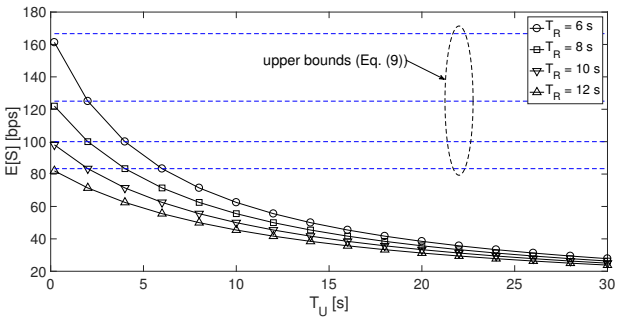


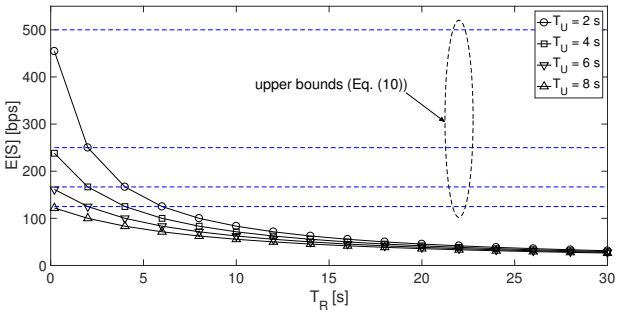
Fig. 4: $E[N]$ versus T_R w.r.t. $k \to 0$.

seconds in respect of the variants of mobility rate $\mu_r \in \{1/6, 1/8, 1/10, 1/12\}$ given a fixed shape parameter $k = 1$, while in Fig. 3(b), T_U is assumed to be in $\{2, 4, 6, 8\}$ seconds. The upper bounds are plotted using (6) and (7) derived in Lemmas 1 and 2, respectively. It can be observed in both Figs. 3(a) and 3(b) that all the simulation results approach the derived bounds and the average NEP increases as either T_U or T_R increases.

Moreover, considering the scenario of a very small shape parameter of gamma distribution, i.e. $k \to 0$, Fig. 4 shows another illustration of the average NEP as a function of the MRI with respect to various values of $k \in \{0.02, 0.05, 0.1\}$. The KUI is set as 2 seconds and other parameters are similarly set as in Fig. 3(b). It can be observed in Fig. 4 that all the NEP curves are lower bounded by (8) and such bound is tighter as k is closer to 0. The above observations accordingly

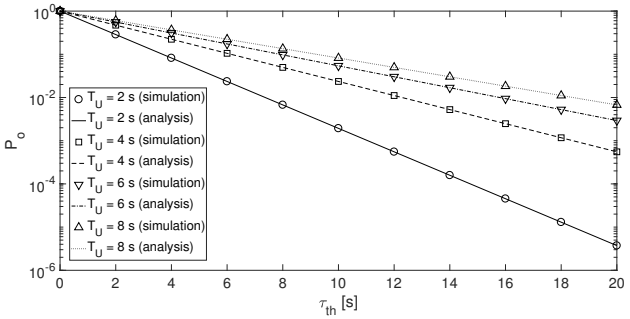


(a)

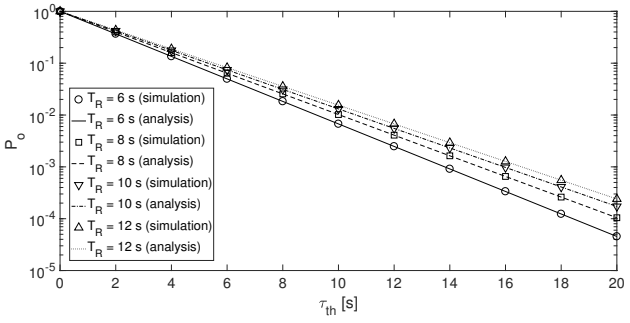


(b)

Fig. 5: (a) $E[S]$ versus T_U w.r.t. T_R; (b) $E[S]$ versus T_R w.r.t. T_U.



(a)



(b)

Fig. 6: OPV versus vulnerable interval threshold w.r.t. (a) T_U; (b) T_R.

verify the statements in Lemmas 1 and 2 regarding the monotonic increase property of $E[N]$ over T_U and T_R as well as confirming the derived bounds of $E[N]$.

B. The impacts of KUI and MRI on SOR Performance

Investigating the impacts of KUI and MRI on the SOR performance, Figs. 5(a) and 5(b) plot the average SOR, i.e. $E[S]$ [bits/s (bps)], versus T_U [s] and T_R [s], respectively. Similar to Fig. 3, T_R is assumed to vary in $\{6, 8, 10, 12\}$ seconds in Fig. 5(a), while in Fig. 5(b), T_U is set in $\{2, 4, 6, 8\}$ seconds. The number of bits for authentication between entities in the network is set as $\rho = 1000$ bits. It can be seen that the average SOR decreases to 0 as either T_U or T_R increases and they are all bounded by (9) and (10) when T_U and T_R approach to 0, respectively. These verify the findings in Lemma 3 about the monotonic decrease property of $E[S]$ over T_U and T_R.

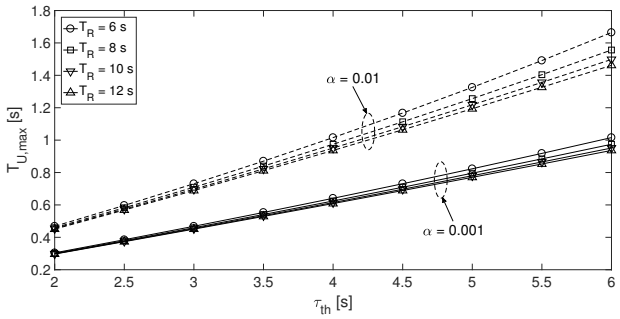
C. The Outage Probability of Vulnerability

Analysing the secrecy performance of MMI handover, Fig. 6 shows the OPV, i.e. P_o as a function of vulnerable interval threshold, i.e. τ_{th}. Specifically, with regard to the KUI and MRI, we assume that T_U varies in $\{2, 4, 6, 8\}$ seconds and $T_R = 8$ seconds in Fig. 6(a), while $T_R \in \{6, 8, 10, 12\}$ seconds and $T_U = 3$ seconds in Fig. 6(b). It can be observed in these figures that an improved performance with a lower OPV is achieved when either the KUI or the MRI is short, which accordingly verifies the statement in Remark 2. Additionally, the analytical results in Lemma 4 with the closed-form expression (17) in Corollary 1 are shown to be consistent with the simulation results.

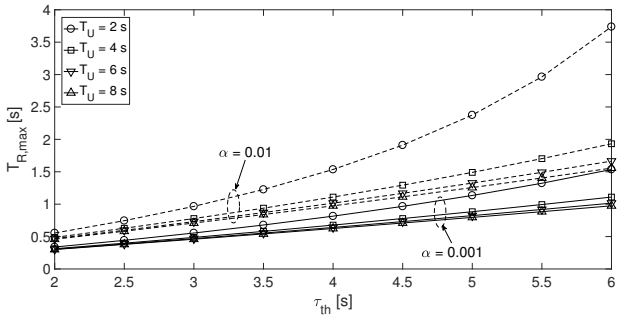
D. Optimal KUI and MRI with FP Approach

In order to find the optimal KUI and MRI that minimise the NEP and SOR subject to OPV constraint, as stated in Lemma 5, we first find the maximal T_U and T_R. Figs. 7(a) and 7(b) plot the maximal T_U, i.e. $T_{U,\max}$, and maximal T_R, i.e. $T_{R,\max}$, respectively, as the functions of the vulnerable interval threshold, i.e. τ_{th}, with respect to two scenarios of OPV constraint $\alpha \in \{0.01, 0.001\}$. In these two subfigures, $T_{U,\max}$ and $T_{R,\max}$ are determined by solving $P_o(x) = \alpha$ where $x \in \{T_U, T_R\}$ and $P_o(x)$ is given by (26). It can be observed that, in order to achieve a stricter OPV requirement with a lower α, either a shorter KUI or MRI is required. This is also reflected from the observation in Fig. 6. Also, in Fig. 7(a), $T_{U,\max}$ is shown to decrease as T_R increases. This is due to the fact that an increased T_R causes a higher OPV and thus T_U should be reduced to achieve the required OPV.

Given the maximal KUI and MRI in Fig. 7 subject to the constraint on the OPV, Figs. 8(a) and 8(b) sequentially plot the optimal values of T_U and T_R, i.e. $T_{U,opt}$ and $T_{R,opt}$, versus the relative importance ratio between NEP and SOR, i.e. δ, using the proposed FP approach. For comparison, an exhaustive search approach in [8] is included in Fig. 8. In this exhaustive search approach, a running step size of 0.05 second is assumed, while in the FP approach, by exploiting the bounds of $E[N]$ and $E[S]$ in Figs. 3 and 5, the normalised NEP and SOR can be determined, and thus the optimal T_R and T_U, i.e. $T_{R,opt}$ and $T_{U,opt}$, can be solved numerically by (31) in Lemma 5. It is assumed that the target maximum OPV is $\alpha = 0.01$ and the vulnerable interval threshold is $\tau_{th} = 5$

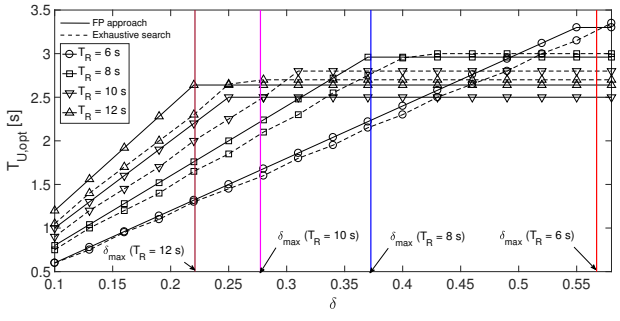


(a)

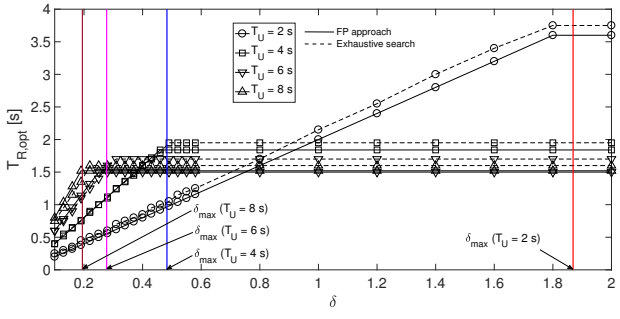


(b)

Fig. 7: (a) Maximal T_U versus τ_{th}; (b) Maximal T_R versus τ_{th}.



(a)



(b)

Fig. 8: (a) Optimal T_U versus δ; (b) Optimal T_R versus δ.

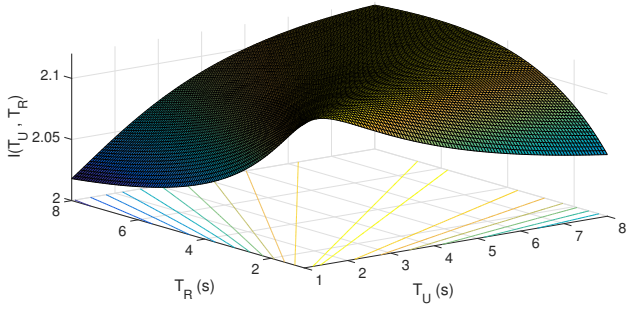


Fig. 9: Reciprocal of weighted sum in MO problem when $w_1 = w_2 = 0.5$.

seconds. As shown in Corollary 2, it is necessary to determine the condition of δ to meet the OPV requirement. Therefore, in Figs. 8(a) and 8(b), the maximal δ, i.e. $\delta_{\max}$, is also illustrated for various scenarios of T_U and T_R.

In Figs. 8(a) and 8(b), it can be seen that $T_{R,opt}$ and $T_{U,opt}$ increase as δ increases up to $\delta_{\max}$. In fact, a higher NEP is required over the SOR to achieve a higher δ. This means the security is of lower priority compared to the signalling overhead. Therefore, the optimal intervals $T_{U,opt}$ and $T_{R,opt}$ must be long enough to provide a lower $E[S]$ while they result in a higher $E[N]$. This observation verifies the notice in Remark 3 regarding the impact of δ as δ varies from 0 to ∞. This also reflects the observations in Figs. 3 and 5 regarding the contradictory between $E[N]$ and $E[S]$ when increasing either T_U or T_R. Furthermore, it can be observed that there is a gap between $T_{U,opt}$ and $T_{R,opt}$ in the proposed FP compared to those in the conventional exhaustive search approach. This accordingly verifies the statement in Remark 4 regarding the effectiveness of the proposed solution in finding the exact optimal values of T_R and T_U over the conventional approach which relies solely on the use of empirical data.

E. Optimal KUI and MRI with FA Approach

Considering the minimisation of the weighted sum of NEP and SOR as shown in (30), we implement FA approach in MATLAB. Note that finding the optimal KUI and MRI is equivalent to finding x and y to maximise the light intensity in FA, i.e. reciprocal of the weighted sum (see (39)). Fig. 9 illustrates the 3-D shaded surface plot of the reciprocal of the weighted sum, i.e. $I(T_U, T_R)$. It is assumed that T_U and T_R vary in the range $[1, 8]$ seconds. Let us consider 20 fireflies, i.e. $N_F = 20$, flying in a 2-D coordinate grid in which the coordinates (x, y) of the fireflies correspond to the values of T_U and T_R to be optimised.

In order to illustrate the operation of the FA in solving the MO problem, Fig. 10 plots the location of 20 fireflies at different stages/generations. The FA is carried out as in Algorithm 2 where the randomisation parameter, the light absorption coefficient and the maximum generation are set as $\varphi = 0.3$, $\gamma = 1$ and $G_{\max} = 50$, respectively. Specifically, in Fig. 10(a), the initial population of fireflies are generated over the 2-D grid with a notice that their location should satisfy the OPV constraint (33) where the the target maximum OPV and

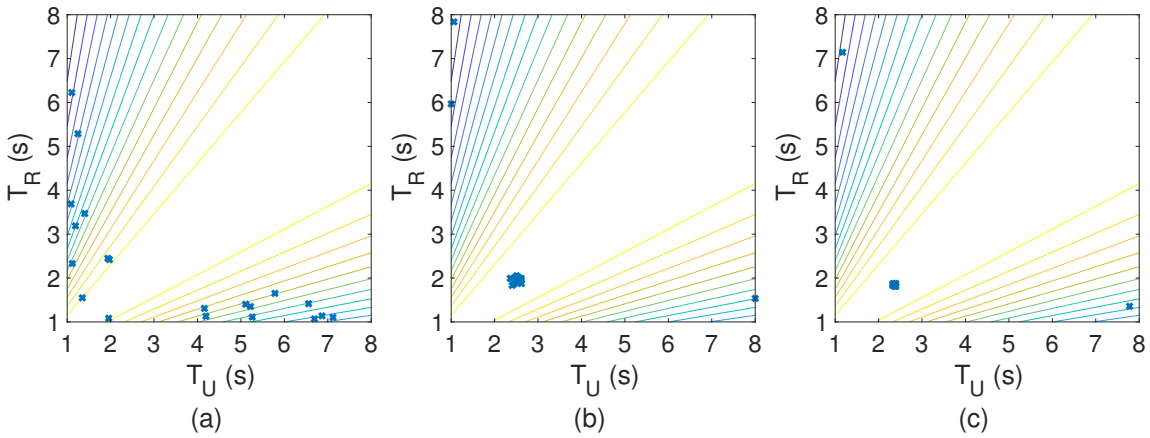


Fig. 10: Location of 20 fireflies: (a) initial population; (b) after 5 generations; and (c) after 50 generations.

the vulnerable interval threshold are $\alpha = 0.01$ and $\tau_{th} = 5$ seconds, respectively. It can be observed in Fig. 10(b) that the fireflies can quickly aggregate in a dense group after only 5 iterations and the optimal location of the firefly having the maximum light intensity can be found after 50 iterations as shown in Fig. 10(c).

A comparison between FP and FA approaches is summarised in Table III where $\alpha \in \{0.1, 0.01\}$ and $\tau_{th} \in \{4, 5, 6, 7, 8\}$ seconds. For fair comparison, it is assumed that $\delta = 1$ in FP method and $w_1 = w_2 = 0.5$ in FA method. The FA is first implemented to find the optimal KUIs and MRIs in different scenarios. Then, for each value of the obtained KUI with the FA, we implement the FP method to find the corresponding optimal MRI. It can be seen that the optimal MRIs are different with 2 approaches; however, they both result in a closed weighted sum of NEP and SOR, i.e. $f(T_U, T_R)$. It is also shown in Table III that both the FP and FA approaches require shorter KUI and MRI for a target OPV, i.e. α, as the vulnerable interval threshold, i.e. τ_{th}, decreases. This is due to the fact that a lower τ_{th} results in a higher OPV (see Fig. 6), and thus, as noted in Remark 2, a shorter KUI and MRI are required to reduce the OPV to achieve its target. Notice that the optimal values in the FA are found so as to minimise the weighted sum of two objectives, while those in the FP are for minimising the fraction of these two objectives. The above observations accordingly verify the effectiveness of the FA in finding the optimal KUIs and MRIs to minimise the weighted sum of two objectives with high reliability and quick convergence.

VIII. Conclusions

In this paper, OPV has been derived along with the bounds of NEP and SOR to not only facilitate the normalisation functions in the optimisation problem but also characterise the monotonicity properties of the NEP, SOR and OPV over the KUI and MRI. It has been shown that the NEP and SOR are respectively increasing and decreasing functions of both the KUI and MRI, while either a short KUI or MRI helps reduce the OPV for an enhanced handover security.

Aiming at minimising the NEP and SOR while still maintaining the OPV constraint, an MO problem has been introduced to find the optimal KUI and MRI to balance these two conflicting objectives. Since there is no single solution to the MO problem with conflicting objectives, it is critical to combine these two objectives into a single objective. Specifically, we have considered two approaches where the objectives can be expressed in the form of either a fraction or a weighted sum.

In the FP approach, the MO problem has been converted to an SO problem where the optimal solutions can be found via a simple numerical method, while in the FA approach, the MO problem has been considered as the minimisation of the weighted sum of the NEP and SOR. Both approaches have shown to provide a lower complexity rather than performing heuristic exhaustive searches. In particular, a quick convergence can be achieved with the FA when the fireflies move quickly towards the optimal values after a small number of generations, and thus is promising to provide a self-adjusting and fast MME handover with enhanced security and lower complexity in practice. A possible extension of this work is to investigate the practical issues of the MME handover key management when employing the proposed approaches to cope with the desynchronisation attacks.

Appendix A
Proof of Lemma 1

From (4), it can be easily shown that $E[N]$ decreases as μ_u increases, and thus $E[N]$ is an increasing function over T_U since $T_U = 1/\mu_u$. The lower bound of $E[N]$ can thus be determined when $T_U \to 0$, i.e. $\mu_u \to \infty$, as

$$\lim_{\mu_u \to \infty} E[N] = 0. \tag{40}$$

The upper bound of $E[N]$ can be computed by applying L'Hospital's Rule when $T_U \to \infty$, i.e. $\mu_u \to 0$. Let us define

$$f_1(\mu_u) \triangleq 1 - \frac{\mu_r}{\mu_u k}\left(1 - \left(\frac{\mu_r}{\mu_u + \mu_r}\right)^k\right), \tag{41}$$

$$g_1(\mu_u) \triangleq \mu_u. \tag{42}$$

TABLE III: Comparison between FP and FA approaches in solving the MO problem

Required OPV i.e. α	**Vulnerable interval threshold** i.e. τ_{th}	**FP Method** with $\delta = 1$ (T_U, T_R)	**FA Method** with $w_1 = w_2 = 0.5$ (T_U, T_R)
$\alpha = 0.1$	$\tau_{th} = 4$s	$(3.09, 3.45)$s	$(3.09, 3.96)$s
	$\tau_{th} = 5$s	$(3.30, 3.68)$s	$(3.30, 4.22)$s
	$\tau_{th} = 6$s	$(4.29, 4.78)$s	$(4.29, 5.49)$s
	$\tau_{th} = 7$s	$(4.33, 4.83)$s	$(4.33, 5.55)$s
	$\tau_{th} = 8$s	$(4.89, 5.45)$s	$(4.89, 6.26)$s
$\alpha = 0.01$	$\tau_{th} = 4$s	$(1.58, 1.76)$s	$(1.58, 2.02)$s
	$\tau_{th} = 5$s	$(1.84, 2.05)$s	$(1.84, 2.36)$s
	$\tau_{th} = 6$s	$(2.30, 2.56)$s	$(2.30, 2.94)$s
	$\tau_{th} = 7$s	$(2.35, 2.62)$s	$(2.35, 3.00)$s
	$\tau_{th} = 8$s	$(2.64, 2.94)$s	$(2.64, 3.38)$s
		$f(T_U, T_R) = 0.4728$	$f(T_U, T_R) = 0.4716$

Substituting (41) and (42) into (4), we have

$$\lim_{\mu_u \to 0} E[N] = \lambda_p \lim_{\mu_u \to 0} \frac{f_1'(\mu_u)}{g_1'(\mu_u)} = \lambda_p \lim_{\mu_u \to 0} f_1'(\mu_u). \tag{43}$$

We continue by calculating $f_1'(\mu_u)$ as follows:

$$\begin{aligned} f_1'(\mu_u) &= \frac{\mu_r}{k\mu_u^2} - \frac{\mu_r^{k+1}}{k} \frac{1}{\mu_u^2 \left(\mu_u + \mu_r\right)^k} - \frac{\mu_r^{k+1}}{\mu_u \left(\mu_u + \mu_r\right)^{k+1}} \\ &\triangleq \frac{f_2(\mu_u)}{g_2(\mu_u)}, \end{aligned} \tag{44}$$

where

$$f_2(\mu_u) = \mu_r \left(\mu_u + \mu_r\right)^{k+1} - \mu_r^{k+1} \left(\mu_u + \mu_r\right) - k\mu_u \mu_r^{k+1}, \tag{45}$$

$$g_2(\mu_u) = k\mu_u^2 \left(\mu_u + \mu_r\right)^{k+1}. \tag{46}$$

Substituting (44) into (43), we then have

$$\lim_{\mu_u \to 0} E[N] = \lambda_p \lim_{\mu_u \to 0} \frac{f_2'(\mu_u)}{g_2'(\mu_u)} = \lambda_p \lim_{\mu_u \to 0} \frac{f_3(\mu_u)}{g_3(\mu_u)}, \tag{47}$$

where

$$f_3(\mu_u) \triangleq (k+1)\mu_r(\mu_u + \mu_r)^k - \mu_r^k, \tag{48}$$

$$g_3(\mu_u) \triangleq k\mu_u(\mu_u + \mu_r)^k \left[2(\mu_u + \mu_r) + (k+1)\mu_u\right]. \tag{49}$$

Similarly, we can arrive at

$$\lim_{\mu_u \to 0} E[N] = \lambda_p \lim_{\mu_u \to 0} \frac{f_3'(\mu_u)}{g_3'(\mu_u)} = \lambda_p \lim_{\mu_u \to 0} \frac{f_4(\mu_u)}{g_4(\mu_u)} \tag{50}$$

where

$$f_4(\mu_u) \triangleq (k+1)\mu_r(\mu_u + \mu_r)^{k-1}, \tag{51}$$

$$\begin{aligned} g_4(\mu_u) \triangleq\ & (\mu_u + \mu_r)^k \left[(k+3)\mu_u + 2\mu_r\right] \\ & + k\mu_u(\mu_u + \mu_r)^{k-1} \left[(k+3)\mu_u + 2\mu_r\right] \\ & + \mu_u(\mu_u + \mu_r)^k(k+3). \end{aligned} \tag{52}$$

Finally, we obtain

$$\lim_{\mu_u \to 0} E[N] = \lambda_p \lim_{\mu_u \to 0} \frac{f_4'(\mu_u)}{g_4'(\mu_u)} = \frac{\lambda_p(k+1)}{2\mu_r}. \tag{53}$$

Equivalently, (40) and (53) can be stated as

$$N_{\min}^{(T_U)} = \lim_{T_U \to 0} E[N] = 0, \tag{54}$$

$$N_{\max}^{(T_U)} = \lim_{T_U \to \infty} E[N] = \frac{\lambda_p(k+1)}{2\mu_r}. \tag{55}$$

Hence, the Lemma is proved.

Appendix B
Proof of Lemma 2

From (4), it can be shown that $E[N]$ increases as either k increases or μ_r decreases. Therefore, $E[N]$ is an increasing function over T_R since $T_R = k/\mu_r$.

Considering both k and μ_r, we have the following cases:

i) $k \to \infty$ *or* $\mu_r \to 0$: we have $T_R \to \infty$, and thus

$$N_{\max}^{(T_R)} = \lim_{k \to \infty} E[N] = \lim_{\mu_r \to 0} E[N] = \frac{\lambda_p}{\mu_u}. \tag{56}$$

ii) $k \to 0$: we have $T_R \to 0$ and

$$N_{\min}^{(T_R)} = \lim_{k \to 0} E[N] = \frac{\lambda_p}{\mu_u} \left(1 - \frac{\mu_r}{\mu_u} \lim_{k \to 0} \frac{f_5(k)}{g_5(k)}\right), \tag{57}$$

where

$$f_5(k) \triangleq 1 - \left(\frac{\mu_r}{\mu_u + \mu_r}\right)^k, \tag{58}$$

$$g_5(k) \triangleq k. \tag{59}$$

It can be seen that $f_5(k) \to 0$ and $g_5(k) \to 0$ as $k \to 0$. By taking the derivative of both $f_5(k)$ and $g_5(k)$ following the L'Hospital's Rule, we can obtain $N_{\min}^{(T_R)}$ as in (8).

iii) $\mu_r \to \infty$: we have $T_R \to 0$ and

$$N_{\min}^{(T_R)} = \lim_{\mu_r \to \infty} E[N] = \frac{\lambda_p}{\mu_u} \left(1 - \frac{1}{k\mu_u} \lim_{\mu_r \to \infty} \frac{f_6(\mu_r)}{g_6(\mu_r)}\right), \tag{60}$$

where $f_6(\mu_r)$ has the same form as $f_5(k)$ in (58) and

$$g_6(\mu_r) = 1/\mu_r. \tag{61}$$

It can be seen that $f_6(\mu_r) \to 0$ and $g_6(\mu_r) \to 0$ as $\mu_r \to \infty$. Similarly, using the L'Hospital's Rule, we can show that $N_{\min}^{(T_R)} = 0$ as $\mu_r \to \infty$.

Summarising the above cases, the Lemma is proved.

Appendix C
Proof of Lemma 4

As described in Section II, the KUI, i.e. t_U, is modeled by an exponential distribution with a rate of μ_u and the MRI, i.e. t_R, is described by a gamma distribution with a shape parameter of k and a rate of μ_r. The cdfs of t_U and t_R are given by [38]

$$F_{t_U}(x) = 1 - e^{-\mu_u x} \tag{62}$$

$$F_{t_R}(x) = \frac{\gamma(k, \mu_r x)}{\Gamma(k)}, \tag{63}$$

respectively, where $\Gamma(z) \triangleq \int_0^\infty e^{-t}t^{z-1}dt,\ \Re\{z\} > 0$, is the gamma function [41, eq. (8.310.1)] and $\gamma(\alpha, z) \triangleq \int_0^z e^{-t}t^{\alpha-1}dt$ is the lower incomplete gamma function [41, eq. (8.350.1)].

Substituting (62) and (63) into (15), we have

$$P_o = \left(1 - \frac{\gamma(k, \mu_r\tau_{th})}{\Gamma(k)}\right) e^{-\mu_u\tau_{th}}. \tag{64}$$

Note that $\gamma(\alpha, z) = \Gamma(\alpha) - \Gamma(\alpha, z)$ [41, eq. (8.356.3)], where $\Gamma(\alpha, z) \triangleq \int_z^\infty e^{-t}t^{\alpha-1}dt$ is the upper incomplete gamma function [41, eq. (8.350.2)]. We can further rewrite (64) as

$$P_o = \frac{\Gamma(k, \mu_r\tau_{th})}{\Gamma(k)} e^{-\mu_u\tau_{th}}. \tag{65}$$

The Lemma is proved.

REFERENCES

[1] F. Khan, *LTE for 4G Mobile Broadband: Air Interface Technologies and Performance*. Cambridge University Press, Apr. 2009.

[2] Q. Xiao, W. Zhou, B. Cui, and L. Li, "An enhancement for key management in LTE/SAE X2 handover based on ciphering key parameters," in *Proc. 3PGCIC 2014*, Guangdong, China, Nov. 2014, pp. 256–261.

[3] M. Gohar and J. G. Choi, "Enhanced mobility management scheme in PMIP-SAE-based mobile networks," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1160–1163, Jun. 2016.

[4] D. Forsberg, "LTE key management analysis with session keys context," *Elsevier Comput. Commun.*, vol. 33, no. 16, pp. 1907–1915, Oct. 2010.

[5] C. B. Sankaran, "Network access security in next-generation 3GPP systems: A tutorial," *IEEE Commun. Mag.*, vol. 47, no. 2, pp. 84–91, Feb. 2009.

[6] P. K. Reddy and B. R. Chandavarkar, "Mitigation of desynchronization attack during inter-eNodeB handover key management in LTE," in *Proc. IC3 2015*, Noida, India, Aug. 2015, pp. 561–566.

[7] S. Mathi and L. Dharuman, "Prevention of desynchronization attack in 4g LTE networks using double authentication scheme," *Procedia Computer Science*, vol. 89, pp. 170–179, 2016.

[8] C.-K. Han and H.-K. Choi, "Security analysis of handover key management in 4G LTE/SAE networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 2, pp. 457–468, Feb. 2014.

[9] S. Tahira, M. Sher, A. Ullah, M. Imran, and A. V. Vasilakos, "Handover based ims registration scheme for next generation mobile networks," *Wireless Communications and Mobile Computing*, vol. 2017, no. 8, p. 16 pages, 2017.

[10] W. Diffie, P. C. Van Oorschot, and M. J. Wiener, "Authentication and authenticated key exchanges," *Designs, Codes and Cryptography*, vol. 2, no. 2, pp. 107–125, Jun 1992.

[11] A. Shaik, R. Borgaonkar, J.-P. Seifert, N. Asokan, and V. Niemi, "Practical attacks against privacy and availability in 4G/LTE," in *Proc. NDSS 2016*, San Diego, California, USA, Feb 2016.

[12] C. M. Moreira, G. Kaddoum, and E. Bou-Harb, "Cross-layer authentication protocol design for ultra-dense 5G HetNets," in *Proc. IEEE ICC 2018*, Kansas City, MO, 2018, pp. 1-7.

[13] A. De Gregorio, "Cryptographic key reliable lifetimes: Bounding the risk of key exposure in the presence of faults," in *Proc. FDTC'06*, Yokohama, Japan, Oct. 2006, pp. 144–158.

[14] S. Pack and W. Lee, "Optimal binding-management-key refresh interval in mobile IPv6 networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 7, pp. 3834–3837, Sep. 2009.

[15] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on threats and attacks on mobile networks," *IEEE Access*, vol. 4, pp. 4543–4572, 2016.

[16] M. Ehrgott, *Multicriteria Optimization*, 2nd ed. Springer, Jun. 2005.

[17] J. Cho, Y. Wang, I. Chen, K. S. Chan, and A. Swami, "A survey on modeling and optimizing multi-objective systems," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1867–1901, thirdquarter 2017.

[18] G. Mavrotas, "Effective implementation of the ϵ-constraint method in multi-objective mathematical programming problems," *Appl. Math. Comput.*, vol. 213, no. 2, pp. 455–465, July 2009.

[19] N. G. Paterakis, M. Gibescu, A. G. Bakirtzis, and J. P. S. Catalão, "A multi-objective optimization approach to risk-constrained energy and reserve procurement using demand response," *IEEE Trans. Power Syst.*, vol. 33, no. 4, pp. 3940–3954, July 2018.

[20] M. Ehrgott and D. M. Ryan, "Constructing robust crew schedules with bicriteria optimization," *Journal of Multi-Criteria Decision Analysis*, vol. 11, no. 3, pp. 139–150, 2002.

[21] K. Klamroth and T. Jørgen, "Constrained optimization using multiple objective programming," *Journal of Global Optimization*, vol. 37, no. 3, pp. 325–355, Mar 2007.

[22] P. N. Ngatchou, A. Zarei, W. L. J. Fox, and M. A. El-Sharkawi, *Pareto Multiobjective Optimization*. John Wiley & Sons, Inc., Jun. 2007, pp. 189–207.

[23] O. Tervo, L. Tran, H. Pennanen, S. Chatzinotas, B. Ottersten, and M. Juntti, "Energy-efficient multicell multigroup multicasting with joint beamforming and antenna selection," *IEEE Trans. Signal Process.*, vol. 66, no. 18, pp. 4904–4919, Sept 2018.

[24] J. G. Lin, "On min-norm and min-max methods of multi-objective optimization," *Math. Program.*, vol. 103, no. 1, pp. 1–33, May 2005.

[25] M. Ehrgott and E. A. Galperin, "Min-max formulation of the balance number in multiobjective global optimization," *Computers & Mathematics with Applications*, vol. 44, no. 7, pp. 899 – 907, 2002.

[26] V. Barichard, M. Ehrgott, X. Gandibleux, and V. T'Kindt, "Multiobjective programming and goal programming: Theoretical results and practical applications," *Springer Publishing Company, Incorporated*, 1st ed., 2009.

[27] M. Tamiz and D. F. Jones, "Goal programming and pareto efficiency," *Journal of Information and Optimization Sciences*, vol. 17, no. 2, pp. 291–307, 1996.

[28] R. A. Loodaricheh, S. Mallick, and V. K. Bhargava, "QoS provisioning based resource allocation for energy harvesting systems," *IEEE Trans. Wireless Commun.* vol. 15, no. 7, pp. 5113–5126, July 2016.

[29] M. Zeleny, "Multiple Criteria Decision Making (MCDM): From paradigm lost to paradigm regained?" *J. Multi-Crit. Decis. Anal.*, vol. 18, pp. 77-89, Oct. 2011.

[30] P. Yu, *Multiple-Criteria Decision Making: Concepts, Techniques, and Extensions*, ser. Mathematical Concepts and Methods in Science and Engineering. Springer US, 2013. [Online]. Available: https://books.google.co.uk/books?id=tMPSBwAAQBAJ

[31] A. P. Wierzbicki, "Reference point methods in vector optimization and decision support," *Working Papers ir98017, International Institute for Applied Systems Analysis*, 1998.

[32] Y. Nikulin, K. Miettinen, and M. M. Mäkelä, "A new achievement scalarizing function based on parameterization in multiobjective optimization," *OR Spectrum*, vol. 34, no. 1, pp. 69–87, Jan 2012.

[33] Q. T. Vien, T. A. Le, X. S. Yang, and T. Q. Duong, "On the handover security key update and residence management in LTE networks," in *Proc. IEEE WCNC 2017*, San Francisco, CA, USA, Mar. 2017, pp. 1–6.

[34] 3GPP TS 36.423, "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); X2 Application Protocol (X2AP)."

[35] Z. Haddad, A. Alsharif, A. Sherif, and M. Mahmoud, "Privacy-preserving intra-MME group handover via MRN in LTE-A networks for repeated trips," in *Proc. IEEE VTC-Fall 2017*, Toronto, ON, Canada, Sept 2017, pp. 1–5.

[36] A. Karandikar, N. Akhtar, and M. Mehta, *Mobility Management in LTE Heterogeneous Networks*, 1st ed. Springer Publishing Company, Incorporated, 2017.

[37] N. Balakrishnan and A. P. Basu, *Exponential Distribution: Theory, Methods and Applications*, 1st ed. New York: CRC Press, 1996.

[38] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*, 4th ed. Mc-Graw Hill, 2002.

[39] M. M. Zonoozi and P. Dassanayake, "User mobility modeling and characterization of mobility patterns," *IEEE J. Sel. Areas Commun.*, vol. 15, no. 7, pp. 1239–1252, Sept 1997.

[40] A. Stuart and J. K. Ord, *Kendall's advanced theory of statistics*, 5th ed. C. Griffin, London, U.K., 1987.

[41] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Academic Press, 2007.

[42] X.-S. Yang, *Firefly Algorithms for Multimodal Optimization*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 169–178.

[43] X.-S. Yang, *Nature-Inspired Metaheuristic Algorithms*. Luniver Press, 2008.

[44] D. E. Goldberg, *Genetic Algorithms in Search, Optimization and Machine Learning*, 1st ed. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1989.

[45] M. Mitchell, *An Introduction to Genetic Algorithms*. Cambridge, MA, USA: MIT Press, 1996.

[46] M. Dorigo, V. Maniezzo, and A. Colorni, "Ant system: optimization by a colony of cooperating agents," *IEEE Trans. Syst., Man, Cybern. B*, vol. 26, no. 1, pp. 29–41, Feb. 1996.
[47] M. Dorigo and T. Stützle, *Ant Colony Optimization*, 1st ed. Scituate, MA, USA: MIT Press, Bradford Company, 2004.
[48] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proc. IEEE International Conference on Neural Networks 1995*, vol. 4, Perth, Australia, Nov. 1995, pp. 1942–1948.
[49] E. Bonabeau, M. Dorigo, and G. Theraulaz, *Swarm Intelligence: From Natural to Artificial Systems*. New York, NY, USA: Oxford University Press, Inc., 1999.
[50] X.-S. Yang, "Firefly algorithm, stochastic test functions and design optimisation," *Int. J. Bio-Inspired Comput.*, vol. 2, no. 2, pp. 78–84, Mar. 2010.
[51] M. K. Marichelvam, T. Prabaharan, and X. S. Yang, "A discrete firefly algorithm for the multi-objective hybrid flowshop scheduling problems," *IEEE Trans. Evol. Comput.*, vol. 18, no. 2, pp. 301–305, Apr. 2014.
[52] X.-S. Yang, S. S. Sadat Hosseini, and A. H. Gandomi, "Firefly algorithm for solving non-convex economic dispatch problems with valve loading effect," *Appl. Soft Comput.*, vol. 12, no. 3, pp. 1180–1186, Mar. 2012.
[53] A. H. Gandomi, X.-S. Yang, and A. H. Alavi, "Mixed variable structural optimization using firefly algorithm," *Computers & Structures*, vol. 89, no. 23-24, pp. 2325–2336, 2011.
[54] X.-S. Yang, S. F. Chien, and T. O. Ting, *Bio-Inspired Computation in Telecommunications*, 1st ed. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2015.

Quoc-Tuan Vien (S'10, M'12, SM'15) received his Ph.D. degree in Telecommunications from Glasgow Caledonian University, U.K., in 2012. He is currently a Senior Lecturer with the Faculty of Science and Technology at Middlesex University, U.K. He has authored a textbook, co-authored five book chapters, and over 80 publications in ISI journals and major conference proceedings. His current research interests include physical-layer security, network coding, non-orthogonal multiple access, RF energy harvesting, device-to-device communications, heterogeneous networks, and Internet of Things. He currently serves as an Editor of the INTERNATIONAL JOURNAL OF DIGITAL MULTIMEDIA BROADCASTING, a Guest Editor of the EAI ENDORSED TRANSACTIONS ON INDUSTRIAL NETWORKS AND INTELLIGENT SYSTEMS, a Program Co-Chair for the EAI International Conference on Industrial Networks and Intelligent Systems (INISCOM 2018, 2019), and a Technical Symposium Co-Chair for the International Conference on Recent Advances in Signal Processing, Telecommunications and Computing (SigTelCom 2017-2019). He was a recipient of the Best Paper Award at the IEEE/IFIP 14th International Conference on Embedded and Ubiquitous Computing in 2016. He was honored as an Exemplary Reviewer of the IEEE COMMUNICATIONS LETTERS in 2017.

Tuan Anh Le (S'10, M'13, SM'19) received his Ph.D. degree in telecommunications research from King's College London, The University of London, U.K., in 2012. From 2009 to 2012, he was a researcher on the Green Radio project funded by the Core 5 joint research program of the U.K.'s Engineering and Physical Sciences Research Council (EPSRC) and the Virtual Center of Excellence in Mobile and Personal Communications (Mobile VCE). From July 2013 to October 2014, he was a Post-Doctoral Research Fellow within the School of Electronic and Electrical Engineering, University of Leeds, Leeds, U.K. In November 2014, he joined the Faculty of Science and Technology, Middlesex University, London, U.K., where he is currently a senior lecturer. His current research interests are RF energy harvesting and wireless power transfer, physical-layer security, robust resource allocation and interference management in 5G cellular networks, channel estimation and resource allocation techniques for massive MIMO, and applied machine learning for wireless communications. He was a recipient of the prestigious Ph.D. scholarship jointly awarded by the Mobile VCE and the U.K. Government's EPSRC. He severed as a Technical Program Chair of the 26th International Conference on Telecommunications (ICT 2019).

Xin-She Yang obtained his DPhil in Applied Mathematics from the University of Oxford. He is now a Reader in Modelling and Optimization at Middlesex University London. Before he joined Middlesex University, he was a Senior Research Scientist at UK's National Physical Laboratory. He is also the IEEE Task Force Chair on Business Intelligence and Knowledge Management, and he has been on the prestigious list of Highly Cited Researchers for consecutive 3 years (2016, 2017, 2018), according to Clarivate Analytics/Web of Science.

Trung Q. Duong (S'05, M'12, SM'13) received his Ph.D. degree in Telecommunications Systems from Blekinge Institute of Technology (BTH), Sweden in 2012. Currently, he is with Queen's University Belfast (UK), where he was a Lecturer (Assistant Professor) from 2013 to 2017 and a Reader (Associate Professor) from 2018. His current research interests include Internet of Things (IoT), wireless communications, molecular communications, and signal processing. He is the author or co-author of over 330 technical papers published in scientific journals (196 articles) and presented at international conferences (135 papers).

Dr. Duong currently serves as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON COMMUNICATIONS, IET COMMUNICATIONS, and a Lead Senior Editor for IEEE COMMUNICATIONS LETTERS. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, IEEE International Conference on Communications (ICC) 2014, IEEE Global Communications Conference (GLOBECOM) 2016, and IEEE Digital Signal Processing Conference (DSP) 2017. He is the recipient of prestigious Royal Academy of Engineering Research Fellowship (2016-2021) and has won a prestigious Newton Prize 2017.